CRITICAL COMMUNICATIONS

IMPLICATIONS FOR 5G

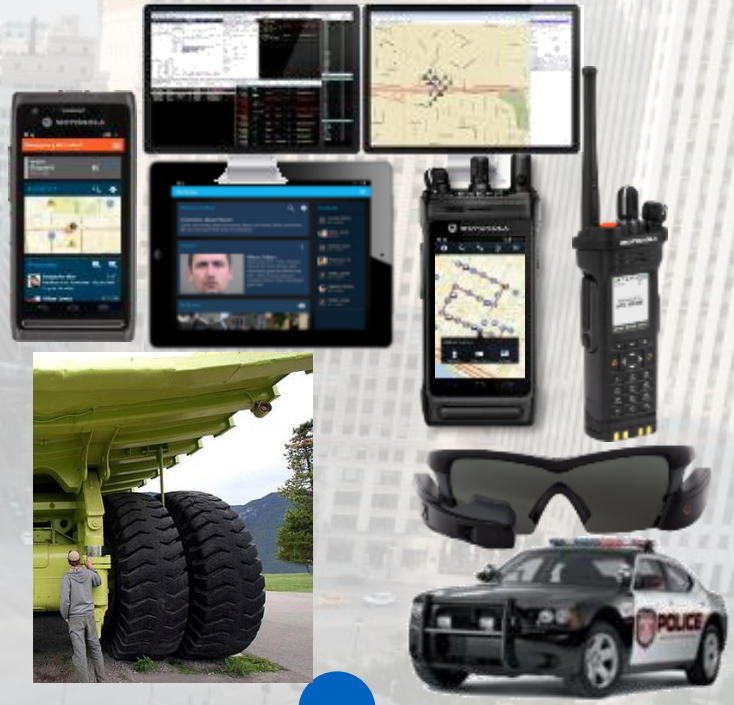
PAUL STEINBERG
CHIEF TECHNOLOGY OFFICER
MOTOROLA SOLUTIONS

BUSINESS/MISSION CRITICAL INTELLIGENCE

ANALOG

DIGITAL

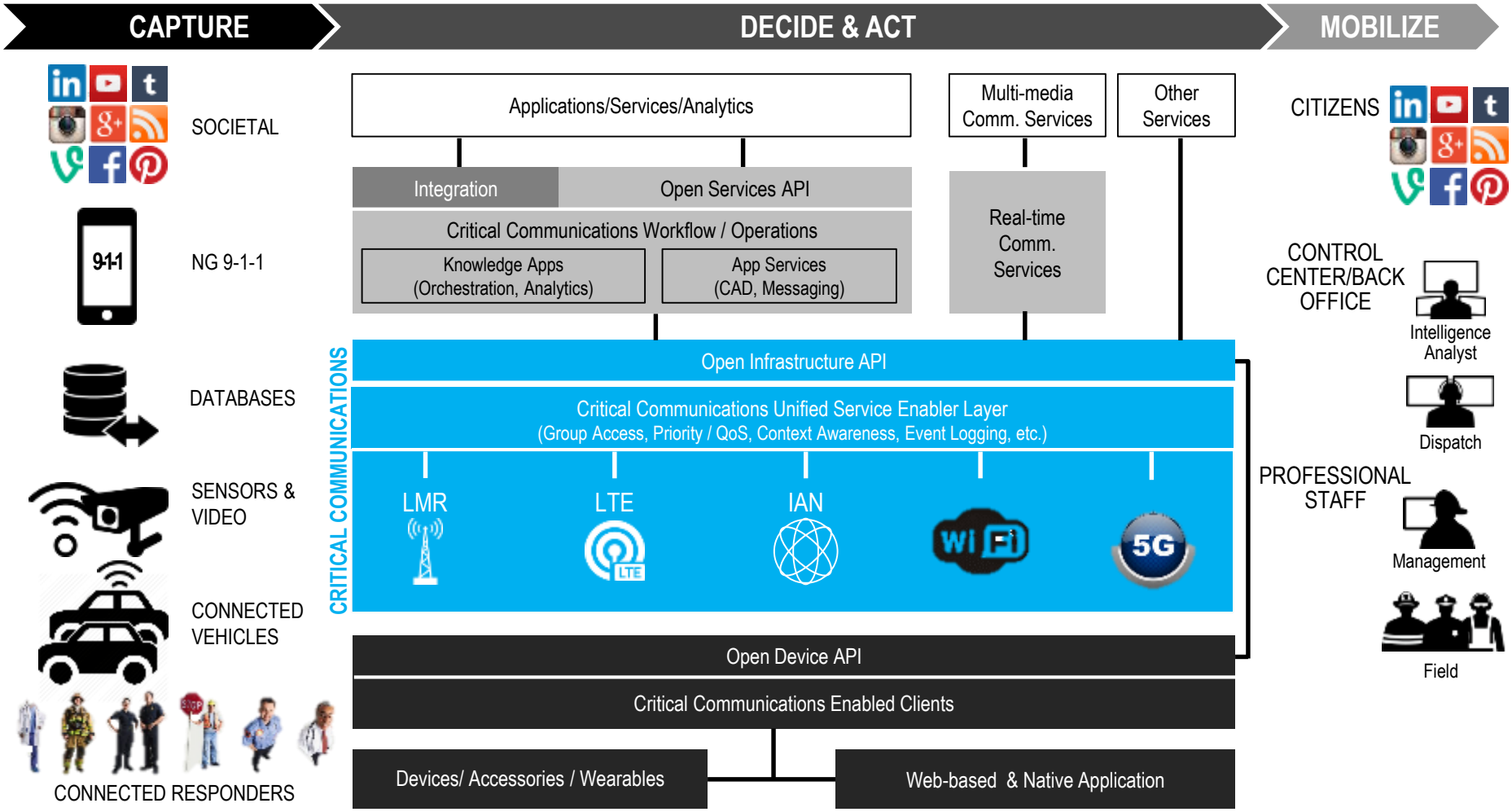
INFORMATION ENABLED



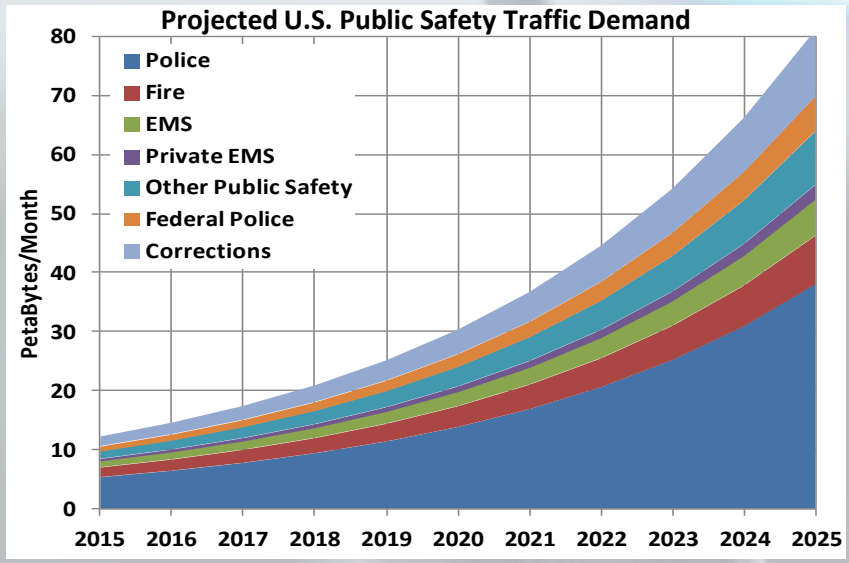
CRITICAL COMMUNICATIONS

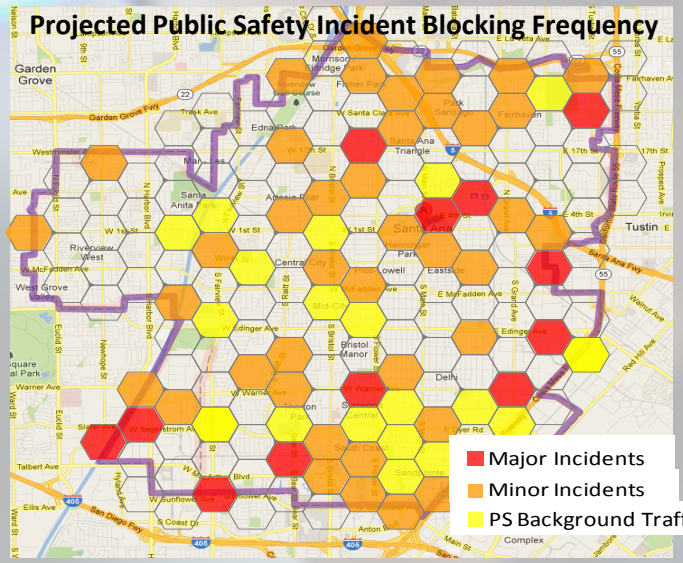
CRITICAL INTELLIGENCE

SOLUTION ARCHITECTURE
CRITICAL INTELLIGENCE



5G CRITICAL COMMUNICATIONS
CAPACITY / COVERAGE / GOS NEEDS





<u>Media Sharing, Virtual Reality, Telepresence & IoT</u> become force multipliers, driving capacity needs with intense periods of high demand in incident scenes, coupled with a need for continual connectivity for IoT, personal communications & secure apps

Critical communications requires <u>secure</u>, <u>highly reliable</u> & <u>ubiquitous coverage</u>, <u>system resilience</u> and <u>graceful degradation</u>

<u>Deployable systems</u> with mesh, ad-hoc and direct mode network topologies needed to fill capacity & coverage gaps

<u>"Security by Design"</u> – security is part of the design process from the beginning

5G CRITICAL COMMUNICATIONS
TECHNOLOGY ELEMENTS

DENSIFICATION

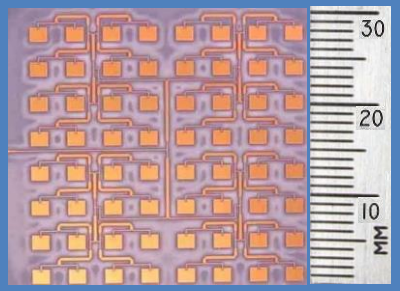
Massive increase in number of devices, sites, backhaul

SDN / NFV

Site density approaching 1 site per active user

Latency reduction

SPECTRUM SHARING



Highly dynamic spectral reuse and interference management

mmWave (>10GHz spectrum with > 1 GHz channels)

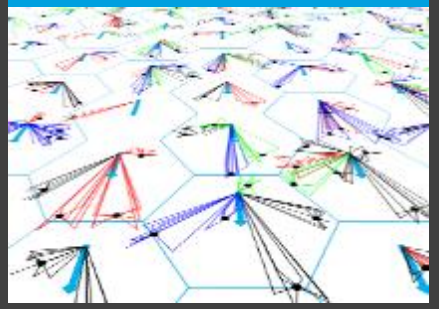
COVERAGE & CAPACITY

Pervasive coverage (95%+) with high minimum throughput

Transparent to broad application ecosystem

Deployable mobile sites, repeaters, relays, ad-hoc and direct modes

SECURITY



5G enables an explosion of interconnected devices, and paradigms broadening the attack surface

Security must be “baked in” 5G standards and 5G devices

5G SMARTER MUST PROVIDE REQUIREMENTS FOCUSED ON BUSINESS/MISSION CRITICAL COMMS

SECURITY & 5G: IOT AS A DRIVER

2015 FCC TAC Cybersecurity WG key findings on IoT

- Perceived gaps:
  - There have been many security gaps publicly identified in existing IoT solutions
  - Many vendors lack knowledge around the secure SW development life cycle (SDLC)
- How industry is addressing these gaps:
  - Many industry orgs provide compliance requirements that includes security
  - Multiple industry best practices include CTA, CSA, NIST, FTC, DHS, OWASP

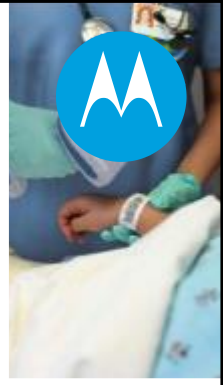
2016 FCC TAC Cybersecurity WG task around 5G Security

- FCC's Goal for the WG
  - Recommend to the FCC the strategy, procedures and steps necessary to help incorporate the concept of "security by design" into the very fabric of 5G
- Proposed scope/direction
  - Leverage the 2015 TAC IoT work and focus on IoT applications of 5G technology
  - Create a list of key security principles that should be built into the 5G IoT ecosystem
  - Identify SDOs and develop an action plan to influence the standards development process

SECURITY & 5G: KEY CONSIDERATIONS

- 5G will enable greater connectivity and an explosion of interconnected devices, broadening the attack surface
- Critical comms, critical infrastructure, ICS, healthcare, etc. drive the need for stronger security capability
- Technical considerations:
  - Protection of dynamic spectrum enablers (e.g. DSA)
  - Privacy enablers (e.g. ephemeral "thing" identifiers)
  - Highly scalable deployment/maintenance models including SDN and NFV
  - Crypto agility for greater interoperability & longevity
  - IoT friendly, decentralized trust models
  - User friendly and interoperable user authentication
  - Rapid defense/response through edge and swarm intelligence

NIST Cyber Security Framework Core Functions



WE INNOVATE TO MOBILIZE AND CONNECT PEOPLE IN THE **MOMENTS THAT MATTER**

MOTOROLA SOLUTIONS